

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 6月24日

出 願 番 号

Application Number:

特願2002-183511

[ ST.10/C ]:

[ JP2002-183511 ]

出 願 人

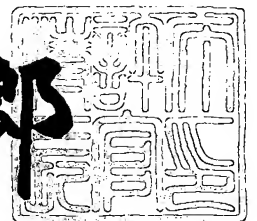
Applicant(s):

インターナショナル・ビジネス・マシーンズ・コーポレーション

2002年11月19日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田 信一郎



出証番号 出証特2002-3091494

【書類名】 特許願

【整理番号】 JP9020102

【提出日】 平成14年 6月24日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 沼尾 雅之

【発明者】

【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 東京基礎研究所内

【氏名】 渡邊 裕治

【特許出願人】

【識別番号】 390009531

【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】 100086243

【弁理士】

【氏名又は名称】 坂口 博

【代理人】

【識別番号】 100091568

【弁理士】

【氏名又は名称】 市位 嘉宏

【代理人】

【識別番号】 100106699

【弁理士】

【氏名又は名称】 渡部 弘道

【復代理人】

【識別番号】 100104880

【弁理士】

【氏名又は名称】 古部 次郎

【手数料の表示】

【予納台帳番号】 081504

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706050

【包括委任状番号】 9704733

【包括委任状番号】 0004480

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報配信システム、そのサーバ及び情報処理装置並びにプログラム

【特許請求の範囲】

【請求項 1】 所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、

前記鍵管理サーバにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末と、

前記公開鍵を用いて所定の属性に対する前記属性秘密鍵を持つ前記ユーザ端末が復号可能な暗号化コンテンツを生成するプロバイダ端末とを備え、

前記プロバイダ端末は、前記暗号化コンテンツを配信し、

前記ユーザ端末は、自分の前記属性秘密鍵にて復号可能な前記暗号化コンテンツを復号することを特徴とする情報配信システム。

【請求項 2】 前記プロバイダ端末は、前記暗号化コンテンツを受信する前記ユーザ端末を指定せずに前記暗号化コンテンツを配信することを特徴とする請求項 1 に記載の情報配信システム。

【請求項 3】 前記ユーザ端末は、前記鍵管理サーバに対して自分の属性を示す属性値の集合を送信し、

前記鍵管理サーバは、管理している前記秘密鍵のうちで、前記ユーザ端末から送信された属性値に対応する秘密鍵に基づいて、当該ユーザ端末に固有の前記属性秘密鍵を生成し、当該ユーザ端末に送信することを特徴とする請求項 1 に記載の情報配信システム。

【請求項 4】 予め定められた所定の属性値に対する秘密鍵及び公開鍵を格納する鍵格納部と、

所定の属性値の集合を取得し、前記鍵格納部に格納されている前記秘密鍵のうちで、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する属性秘密鍵生成部と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵生成部にて生成された前記属性秘密鍵を当該ユーザ端末に

送信する送受信部と

を備えることを特徴とするサーバ。

【請求項 5】 前記属性秘密鍵生成部は、オブビリアス・トランスファーを実現するプロトコルを用いて前記属性秘密鍵を生成することを特徴とする請求項 4 に記載のサーバ。

【請求項 6】 コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する条件鍵生成部と、

前記条件鍵に基づいて前記コンテンツを暗号化する暗号化コンテンツ生成部と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する送信部と

を備えることを特徴とする情報処理装置。

【請求項 7】 前記条件鍵生成部は、個々の属性値に対する公開鍵を用いて暗号化された当該属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、前記コンテンツの送信先を制限する条件鍵を生成することを特徴とする請求項 6 に記載の情報処理装置。

【請求項 8】 前記条件鍵生成部は、前記コンテンツを暗号化するためのセッション鍵と当該セッション鍵を復号するための条件鍵とを生成し、

前記暗号化コンテンツ生成部は、前記セッション鍵を用いて前記コンテンツを暗号化することを特徴とする請求項 6 に記載の情報処理装置。

【請求項 9】 ネットワークを介して配信されるコンテンツを受信する情報処理装置において、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する送受信部と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する復号処理部と

を備えることを特徴とする情報処理装置。

【請求項 1 0】 前記送受信部は、自装置に関して設定された属性を示す属性値の集合を前記鍵管理サーバに送信し、当該属性値の集合に基づいて生成された前記属性秘密鍵を当該鍵管理サーバから受信することを特徴とする請求項 9 に記載の情報処理装置。

【請求項 1 1】 コンピュータを制御して、所定の公開鍵で暗号化された情報を復号する復号鍵を生成するプログラムであって、

予め定められた所定の属性値に対する秘密鍵及び公開鍵を所定の記憶装置に格納する機能と、

所定の属性値の集合を取得し、前記記憶装置に格納されている前記秘密鍵のうちで、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する機能と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵を当該ユーザ端末に送信する機能と

を前記コンピュータに実現させることを特徴とするプログラム。

【請求項 1 2】 前記プログラムにより実現される前記属性秘密鍵を生成する機能は、オブビリアス・トランスファーを実現するプロトコルを用いて前記属性秘密鍵を生成することを特徴とする請求項 1 1 に記載のプログラム。

【請求項 1 3】 コンピュータを制御して、所定のコンテンツを暗号化し配信するプログラムであって、

コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する機能と、

前記条件鍵に基づいて前記コンテンツを暗号化する機能と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する機能と

を前記コンピュータに実現させることを特徴とするプログラム。

【請求項 1 4】 前記プログラムにより実現される前記条件鍵を生成する機能は、個々の属性値に対する公開鍵を用いて暗号化された当該属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、前記コンテンツの送

信先を制限する条件鍵を生成することを特徴とする請求項 1 3 に記載のプログラム。

【請求項 1 5】 コンピュータを制御して、ネットワークを介して配信されるコンテンツを受信するプログラムであって、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する機能と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する機能とを前記コンピュータに実現させることを特徴とするプログラム。

【請求項 1 6】 コンピュータを制御して所定の公開鍵で暗号化された情報を復号する復号鍵を生成するプログラムを、当該コンピュータが読み取り可能に格納した記録媒体であって、

前記プログラムは、

予め定められた所定の属性値に対する秘密鍵及び公開鍵を所定の記憶装置に格納する機能と、

所定の属性値の集合を取得し、前記記憶装置に格納されている前記秘密鍵のうち、当該属性値に対応する秘密鍵に基づいて、当該属性値の集合に対応する属性秘密鍵を生成する機能と、

ネットワークを介して、所定のユーザ端末から前記属性値の集合を受信すると共に、前記属性秘密鍵を当該ユーザ端末に送信する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

【請求項 1 7】 コンピュータを制御して所定のコンテンツを暗号化し配信するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、当該公開鍵を用いて当該公開鍵に対応する秘密鍵で復号される条件鍵を生成する機能と、

前記条件鍵に基づいて前記コンテンツを暗号化する機能と、

ネットワークを介して、前記コンテンツの送信先を指定せずに暗号化された前記コンテンツを送信する機能と

を前記コンピュータに実現させることを特徴とする記録媒体。

【請求項 1 8】 コンピュータを制御してネットワークを介して配信されるコンテンツを受信するプログラムを、当該コンピュータが読み取り可能に記録した記録媒体であって、

前記プログラムは、

所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、当該秘密鍵に基づいて生成され、自装置に関して設定された属性に対応した属性秘密鍵を受信する機能と、

暗号化されたコンテンツを取得し、前記属性秘密鍵に基づいて復号する機能とを前記コンピュータに実現させることを特徴とする記録媒体。

【請求項 1 9】 コンピュータを制御して、所定の公開鍵で暗号化された情報を復号する復号鍵を生成し配布する鍵配布方法において、

$n$  個の秘密鍵及び当該秘密鍵に対応する  $n$  個の公開鍵を生成し、所定の記憶装置に格納するステップと、

前記記憶装置に格納された  $n$  個の秘密鍵のうち、所定のクライアントにより任意に選択された  $k$  ( $\leq n$ ) 個の秘密鍵に関する情報を取得するステップと、

取得した秘密鍵に関する情報に対応する  $k$  個の前記秘密鍵を前記記憶装置から読み出し、オブビリアス・トランスファーを実現するプロトコルを用いて、当該  $k$  個の秘密鍵に対応する  $k$  個の前記公開鍵で暗号化された情報を復号する復号鍵を生成するステップと、

生成された前記復号鍵を前記クライアントに提供するステップと

を含むことを特徴とする鍵配布方法。

【請求項 2 0】 所定の属性値に対する秘密鍵及び公開鍵を管理するサービスプロバイダと、

前記サービスプロバイダにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備え、

所定の前記ユーザ端末は、前記公開鍵を用いて所定の属性に対する前記属性秘



密鍵を持つ前記ユーザ端末が復号可能な暗号化コンテンツを生成して、他のユーザ端末に送信し、

前記他のユーザ端末は、自分の前記属性秘密鍵にて復号可能な前記暗号化コンテンツを復号することを特徴とする情報配信システム。

【請求項 2 1】 所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、

前記鍵管理サーバにアクセスし、前記秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備え、

所定の前記ユーザ端末は、前記公開鍵を用いて所定の属性に対する前記属性秘密鍵を持つ前記ユーザ端末が復号可能なグループ鍵を生成して他のユーザ端末に送信し、当該グループ鍵により利用が可能となるコンテンツをネットワーク上に設置することを特徴とする情報配信システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データベース検索システムに関し、特に所定のデータベースが所定のデータを保有しているか否かを検索するシステムに関する。

【 0 0 0 2 】

【従来の技術】

データ通信では、通常、コンテンツの宛先として受信者のアドレスを指定する必要がある、「このような人」というように受信者の属性を指定してコンテンツを送信することはできない。反対に、マルチキャスト（同報通信）の場合、受信者側で送信者（マルチキャストアドレス）を指定してコンテンツを受信することができるが、これも受信者の属性によって受信の可否を指定できるものではない。

【 0 0 0 3 】

今日、パーソナライズされた情報（宣伝）が求められており、個人の属性にあった情報の受け渡しが要求される場面も多い。受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を

満たす人のみが受信できるようなコンテンツ配信システムの実現が望まれている。例えば、条件として〔性別＝男、年齢＝30歳以上、職業＝会社員、趣味＝旅行〕のようなものが記述でき、予めこの条件を満たすような属性を登録しておいた受信者が、コンテンツを受信できるようなシステムである。

一方、プライバシーの問題も重要であり、個人の属性はまさに保護されるべき情報になっている。

#### 【0004】

認証およびパーソナライゼーションのための属性管理システムとして代表的なものに、米国マイクロソフト社のPassport [MS Passport] がある。このシステムは、1つのサーバにおいて、口座番号などのユーザの個人情報をすべて管理し、ユーザの承認を前提として、サーバ側にこれを提供しようとするものである。情報は暗号化して送られる。

#### 【0005】

##### 【発明が解決しようとする課題】

しかし、上述した米国マイクロソフト社のPassportに代表される従来の属性管理システムは、個人情報を全て管理するサーバを前提としているため、利用者は、このサーバ（及びその管理者）を全面的に信頼せざるを得ないという問題がある。すなわち、サーバが不正に個人情報を漏洩しようとする場合、利用者はこれを阻止することができない。

また、セキュリティにおいても、当該サーバのみを攻撃対象とすることができ、すなわちシングルアタックポイントになっているため、たとえ運用上の管理が適切であっても、外部の攻撃によって、個人情報が流出する危険性がある。

#### 【0006】

そこで、本発明は、受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムにおいて、コンテンツの受け渡しに関わる全ての過程で、個人の属性情報が、送信者も含めた第三者には漏れないようにすることを目的とする。

#### 【0007】

## 【課題を解決するための手段】

上記の目的を達成する本発明は、次のように構成されたことを特徴とする情報配信システムとして実現される。この情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、この鍵管理サーバにアクセスし、秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末と、公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能な暗号化コンテンツを生成するプロバイダ端末とを備え、このプロバイダ端末は、暗号化コンテンツを配信し、ユーザ端末は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号することを特徴とする。

## 【0008】

より詳細には、この鍵管理サーバは、予め定められた所定の属性値に対する秘密鍵及び公開鍵を格納する鍵格納部と、所定の属性値の集合を取得し、鍵格納部に格納されている秘密鍵のうちで、この属性値に対応する秘密鍵に基づいて、この属性値の集合に対応する属性秘密鍵を生成する属性秘密鍵生成部と、ネットワークを介して、所定のユーザ端末からこの属性値の集合を受信すると共に、属性秘密鍵生成部にて生成された属性秘密鍵をこのユーザ端末に送信する送受信部とを備える。

## 【0009】

また、このプロバイダ端末は、コンテンツを送信する相手の属性を示す属性値に対する公開鍵を取得し、公開鍵を用いて公開鍵に対応する秘密鍵で復号される条件鍵を生成する条件鍵生成部と、条件鍵に基づいてコンテンツを暗号化する暗号化コンテンツ生成部と、ネットワークを介して、コンテンツの送信先を指定せずに暗号化されたコンテンツを送信する送信部とを備える。

ここで、この条件鍵生成部は、個々の属性値に対する公開鍵を用いて暗号化された、この属性値に対応する条件鍵を、所定の規則に基づいて組み合わせることにより、コンテンツの送信先を制限する条件鍵を生成する。

## 【0010】

さらに、このユーザ端末は、所定の属性値に対応する秘密鍵及び公開鍵を管理する鍵管理サーバにアクセスし、この秘密鍵に基づいて生成され、自装置に関し

て設定された属性に対応した属性秘密鍵を受信する送受信部と、暗号化されたコンテンツを取得し、属性秘密鍵に基づいて復号する復号処理部とを備える。

ここで、この送受信部は、自装置に関して設定された属性を示す属性値の集合を鍵管理サーバに送信し、この属性値の集合に基づいて生成された属性秘密鍵をこの鍵管理サーバから受信する。

#### 【 0 0 1 1 】

また、本発明は、コンピュータを制御して、上述した鍵管理サーバやプロバイダ端末、ユーザ端末として機能させるプログラムとして実現することができる。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

#### 【 0 0 1 2 】

さらに、本発明は、次のような具体的な情報配信システムとして実現される。すなわち、この情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理するサービスプロバイダと、このサービスプロバイダにアクセスし、この秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備える。そして、所定のユーザ端末は、この公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能な暗号化コンテンツを生成して、他のユーザ端末に送信し、かかる他のユーザ端末は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号することを特徴とする。

あるいは、本発明による他の情報配信システムは、所定の属性値に対する秘密鍵及び公開鍵を管理する鍵管理サーバと、この鍵管理サーバにアクセスし、この秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得した複数のユーザ端末とを備える。そして、所定のユーザ端末は、この公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末が復号可能なグループ鍵を生成して他のユーザ端末に送信し、このグループ鍵により利用が可能となるコンテンツをネットワーク上に設置する。

#### 【 0 0 1 3 】

#### 【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。

図 1 は、本実施の形態による情報配信システムの概略構成を説明する図である。

図 1 を参照すると、本実施の形態の情報配信システムは、属性の指定に用いられる属性鍵を管理する属性鍵管理サーバ 10 と、コンテンツ（情報）の送信者であるプロバイダ端末 20 と、コンテンツの受信者であるユーザ端末 30 とを備える。

本実施の形態において、属性鍵管理サーバ 10、プロバイダ端末 20 及びユーザ端末 30 は、ワークステーションやパーソナルコンピュータ、その他のネットワーク機能を備えたコンピュータ装置にて実現される。また、ユーザ端末 30 は、PDA (personal digital assistants) や携帯電話などのネットワーク機能を備えた情報端末装置にて実現することもできる。

これらの装置は、図示しないネットワークを介してデータ交換を行う。ネットワークの通信回線は有線であると無線であるを問わない。

#### 【 0 0 1 4 】

図 6 は、本実施の形態による属性鍵管理サーバ 10、プロバイダ端末 20 及びユーザ端末 30 を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示した図である。

図 6 に示すコンピュータ装置は、演算手段である CPU (Central Processing Unit: 中央処理装置) 101 と、M/B (マザーボード) チップセット 102 及び CPU バスを介して CPU 101 に接続されたメインメモリ 103 と、同じく M/B チップセット 102 及び AGP (Accelerated Graphics Port) を介して CPU 101 に接続されたビデオカード 104 と、PCI (Peripheral Component Interconnect) バスを介して M/B チップセット 102 に接続されたハードディスク 105、ネットワークインターフェイス 106 及び USB ポート 107 と、さらにこの PCI バスからブリッジ回路 108 及び ISA (Industry Standard Architecture) バスなどの低速なバスを介して M/B チップセット 102 に接続されたフロッピーディスクドライブ 109 及びキーボード/マウス 110 とを備える。

なお、図 1 は本実施の形態を実現するコンピュータ装置のハードウェア構成を例示するに過ぎず、本実施の形態を適用可能であれば、他の種々の構成を取ることができる。例えば、ビデオカード 1 0 4 を設ける代わりに、ビデオメモリのみを搭載し、CPU 1 0 1 にてイメージデータを処理する構成としても良いし、ATA (AT Attachment) などのインターフェイスを介して CD-ROM (Compact Disc Read Only Memory) や DVD-ROM (Digital Versatile Disc Read Only Memory) のドライブを設けても良い。

## 【 0 0 1 5 】

図 1 において、プロバイダ端末 2 0 は、コンテンツの送信先を特定するための属性を指定して、当該コンテンツをユーザ端末 3 0 に送信する。この属性を指定するために属性鍵管理サーバ 1 0 が提供する属性鍵が使用される。属性鍵とは、プロバイダ端末 2 0 からユーザ端末 3 0 への通信において指定し得る属性に対して設定された鍵（秘密鍵及び公開鍵）である。また、ユーザ端末 3 0 は、属性鍵管理サーバ 1 0 から自分の属性に対する属性鍵を取得していれば良く、その数は不特定である。したがって、プロバイダ端末 2 0 は、各ユーザ端末 3 0 に対してマルチキャスト（同報通信）によりコンテンツを送信する。

## 【 0 0 1 6 】

本実施の形態において、属性および属性の取り得る値（属性値）は、予め決められているものとする。ここで、属性とは、ユーザ端末 3 0 のユーザやユーザ端末 3 0 自体の個性を表す情報であり、本実施の形態が利用されるシステムの態様や運用に応じて種々の情報を属性として定めることができる。また、所定の属性  $A_i$  に対して、 $V_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,n}\}$  が取り得る値の集合（サイズ =  $n_i$ ）だとする。さらに複数の値を取り得るような属性もあることから、これを一般化して  $k_i$  ( $\leq n_i$ ) 個の値を取ることができるものとする。これらは、属性に固有のものとする。例えば、属性  $A_1$  が性別だとすると  $V_1$  {男、女} で  $n_1 = 2$ 、 $k_1 = 1$  となる。

属性条件は、以下のように記述する。ある属性  $A_i$  の属性値が  $v_i$  であることを  $A_i(v_i)$  と書く。さらに、AND、OR のオペレータ（演算子）として &、| および括弧 ( ) を使うことにする。例えば、

{性別＝男、年齢＝30代、職業＝会社員、趣味＝旅行またはパソコン}

という属性は、

性別（男）&年齢（30代）&職業（会社員）&（趣味（旅行）|趣味（パソコン））

と記述される。

また、以下の説明において、 $p$  は大きな素数、 $q$  は  $p-1$  を割り切るような素数、 $g$  は有限体  $Z_p$  上の位数  $q$  の元とする。また、特に断らない限り全ての計算は  $Z_p$  上で行われるとする。

【0017】

図2は、本実施の形態における属性鍵管理サーバ10、プロバイダ端末20及びユーザ端末30の構成を示す図である。

図2を参照すると、属性鍵管理サーバ10は、属性鍵を生成する属性鍵生成部11と、生成された属性鍵を格納する属性鍵格納部12とを備える。ここで、属性鍵生成部11は、属性鍵として予め定められた個々の属性に対する秘密鍵及び公開鍵を生成すると共に、個々のユーザ端末30との情報のやりとりを通じて当該ユーザ端末30の個別の属性に対応する秘密鍵（属性秘密鍵）を生成する。生成されたユーザ端末30に固有の属性秘密鍵は、該当するユーザ端末30に送られる。

この属性鍵生成部11は、属性鍵管理サーバ10を構成するコンピュータ装置におけるプログラム制御されたCPU101にて実現される仮想的なソフトウェアブロックである。属性鍵格納部12は、属性鍵管理サーバ10を構成するコンピュータ装置の記憶装置（磁気ディスク装置や光ディスク装置、半導体メモリなど）にて実現される。また、特に図示しないが、属性鍵管理サーバ10は、プログラム制御されたCPU101及びネットワークインターフェイス106にて実現される送受信部を備える。

【0018】

プロバイダ端末20は、配信するコンテンツを暗号化する暗号化コンテンツ生成部21と、暗号化されたコンテンツを復号するために用いられる条件鍵を生成する条件鍵生成部22とを備える。ここで、暗号化コンテンツ生成部21は、セ

セッション鍵と呼ばれる共通鍵を用いてコンテンツ自体を暗号化する。これに対し、条件鍵生成部 2 2 は、コンテンツを直接復号する鍵を生成するのではなく、セッション鍵を暗号化し当該セッション鍵を復号するための情報を含む鍵を条件鍵として生成する。

この暗号化コンテンツ生成部 2 1 及び条件鍵生成部 2 2 は、プロバイダ端末 2 0 を構成するコンピュータ装置におけるプログラム制御された CPU 1 0 1 にて実現される仮想的なソフトウェアブロックである。また、特に図示しないが、プロバイダ端末 2 0 は、プログラム制御された CPU 1 0 1 及びネットワークインターフェイス 1 0 6 にて実現される送受信部を備える。

#### 【 0 0 1 9 】

ユーザ端末 3 0 は、属性鍵管理サーバ 1 0 から取得した当該ユーザ端末 3 0 に固有の属性秘密鍵を保持する属性秘密鍵格納部 3 1 と、属性秘密鍵格納部 3 1 に格納された属性秘密鍵を用いてプロバイダ端末 2 0 から配信された暗号化コンテンツを復号する復号処理部 3 2 とを備える。

属性秘密鍵格納部 3 1 は、ユーザ端末 3 0 を構成するコンピュータ装置や情報端末装置の記憶装置（磁気ディスク装置や光ディスク装置、半導体メモリなど）にて実現される。復号処理部 3 2 は、プログラム制御された CPU 1 0 1 にて実現される仮想的なソフトウェアブロックである。また、特に図示しないが、ユーザ端末 3 0 は、プログラム制御された CPU 1 0 1 及びネットワークインターフェイス 1 0 6 にて実現される送受信部を備える。

#### 【 0 0 2 0 】

次に、本実施の形態による情報配信システムを実現するために用いられるプロトコルを説明する。

本実施の形態にて用いられるプロトコルは、

1. 事前処理としての属性鍵の生成と配布、
2. プロバイダ端末 2 0 による条件鍵の生成、
3. マルチキャストによるコンテンツの配信、

の 3 つを含む。以下、それぞれについて詳細に説明する。

#### 【 0 0 2 1 】



## 1. 属性鍵生成と鍵配布

属性鍵管理サーバ 10 の属性鍵生成部 11 は、登録された属性  $A_i$  に対する属性値の集合  $\{v_{i,1}, v_{i,2}, \dots, v_{i,n}\}$  の各々の値に対して、属性秘密鍵  $s_{i,j}$  をランダムに選び、さらに属性公開鍵

【数 1】

$$y_{i,j} = g^{s_{i,j}} \pmod{p}$$

を公開する。

【0022】

ユーザ端末 30 は、属性鍵管理サーバ 10 との間で通信を行い、オブビリアス・トランスファー (Oblivious Transfer: 以下、OT と略す) を行うことによって、自分の属性値に対する属性秘密鍵を属性鍵管理サーバ 10 にも知られることなく取得する。ここで、OT とは、情報提供者と選択者の 2 人の間のプロトコルであり、提供者が持つ複数個の情報のうち、いくつかを選択者が選んで得るというものである。この時、以下の 2 つの条件が満たされなければならない。

(1) 選択者のプライバシー: 提供者は選択者がどれを選んだかを知ることができない。

(2) 提供者のプライバシー: 選択者は選んだ情報以外を知ることとはできない。

なお、OT については次の文献に詳細に開示されている。

文献: M. Bellare and S. Micali, Non-interactive oblivious transfer and applications, Advances in Cryptology - Crypto '89, pp. 547-557, 1990.

【0023】

基本的な OT として 1-out-of-2-OT がある。これは、提供者が 2 つの情報を持ち、選択者はそのうちの 1 つを選ぶというものである。これを実現する代表的なプロトコルは ElGamal 暗号を使ったものがある。以下に、このプロトコルを示す。ここで、提供者の持つ情報を  $I_0, I_1$  とし、選択者の選択値を  $b \in \{0, 1\}$

、 $\sim b = \text{NOT } b$ とする。

(1) 情報提供者が、乱数  $r$  を生成し、選択者へ送信。

(2) 選択者が、受信した乱数  $r$  を用いて  $K_b = g^x$ 、 $K_{-b} = r / K_b$  を生成し、情報提供者へ送信。

(3) 情報提供者が、 $K_0 * K_1 = r$  をチェック。

(4) 情報提供者が、暗号化コンテンツ  $\{E_{I1}, E_{I2}\}$  を生成し、選択者へ送信。ここで、 $E_{I1} = (g^h, I_0 * K_0^h)$ 、 $E_{I2} = (g^h, I_1 * K_1^h)$  である。

(5) 選択者が、コンテンツ  $I_b$  を復号。

#### 【0024】

以上説明した1-out-of-2-OTは、2つの情報の中からいずれか1つを選ぶプロトコルであったが、本実施の形態では、これを拡張して  $n$  個の情報の中から任意の  $k$  個の情報を選ぶ  $k$ -out-of- $n$ -OT を実行する。このプロトコルについて、図3を参照して詳細に説明する。

属性  $A_i$  の属性値数が  $n$  で、選択可能数が  $k$  であるものとする。

(1) 属性鍵管理サーバ10は、予め秘密の値  $t_0$  を決め、

#### 【数2】

$$Q_0 = g^{t_0} \pmod{p}$$

を公開しておく。

(2) ユーザ端末30は、 $k$  個の秘密鍵  $\{t_1, t_2, \dots, t_k\}$  をランダムに決め、その公開鍵

#### 【数3】

$$Q_i = g^{t_i} \pmod{p}$$

を計算する。 $n$  個の属性値の集合  $\{v_{i,1}, v_{i,2}, \dots, v_{i,n}\}$  の中から選  
び出した  $k$  個の集合  $\{v_{i,h(1)}, v_{i,h(2)}, \dots, v_{i,h(k)}\}$  が自分の属性だ  
とする。 $k+1$  個の点  $\{(0, Q_0), (h(1), Q_1), \dots, (h(k), Q_k)\}$

),  $Q_k$ ) } を通るような  $k$  次多項式  $Y(x)$  は、ラグランジュの補間法を使えば一意に決められる。この多項式を使って  $n$  個の点  $\{Y(1), Y(2), \dots, Y(n)\}$  を属性鍵管理サーバ 10 に送信する (秘密通信路を用いる必要はない)。

(3) 属性鍵管理サーバ 10 の属性鍵生成部 11 は、ユーザ端末 30 の公開している (ユーザ端末 30 から送信された)  $n$  個の点が  $k$  次多項式上の点であることを以下の方法で検証した後、正しく  $k$  次多項式上の点であるならば、 $Y(j)$  をそれぞれ  $E1Gamma1$  暗号の公開鍵として、属性秘密鍵  $s_{ij}$  を暗号化したものをユーザ端末 30 に送信する (秘密通信路を用いる必要はない)。

( $n$  点が  $k$  次多項式上の点であることの検証)

「 $n$  個の点集合  $U_1, \dots, U_n$  から  $k+1$  個の点をランダムに選んだ 2 つの集合  $S_1$  と  $S_2$  を  $S_1 \cup S_2 = U_n$  になるように作る。それぞれのセットから  $k$  次多項式を構成し、それらが等しいことを検証する。」

(4) ユーザ端末 30 は、属性鍵管理サーバ 10 から受信した、暗号化された属性秘密鍵  $s_{ij}$  を用いて、 $h(j)$  ( $1 \leq j \leq k$ ) によって指定された  $k$  個の点の  $E1Gamma1$  暗号文のみを復号できる。すなわち、 $k$  個の属性秘密鍵を得ることができた。

#### 【0025】

また、数値属性に対する属性秘密鍵は、上記の  $k$ -out-of- $n$ -OT とは別に、次のような表現を用いて生成される。

(1)  $n$  ビットの正整数  $x$  のバイナリ表現を  $(x_{n-1}, \dots, x_0)$  とする。

(2) 属性鍵管理サーバ 10 の属性鍵生成部 11 は、 $2n$  組の秘密鍵・公開鍵のペア  $\{(pk_j^{(0)}, sk_j^{(0)}), (pk_j^{(1)}, sk_j^{(1)})\}$  ( $j=0, \dots, n-1$ ) を生成し、各桁に対して、2 種類の秘密鍵を割り当てる。すなわち、 $j$  桁目に対して、 $sk_j^{(0)}$  と  $sk_j^{(1)}$  を割り当てる。これに対応する公開鍵  $pk_j^{(0)}$ ,  $pk_j^{(1)}$  は公開する。

(3) 既存の手法である 1-out-of-2 OT による属性鍵配布により、値  $X = (x_{n-1}, \dots, x_0)$  を選択したユーザ端末 30 は、 $(sk_j^{(x_{n-1})}, \dots, sk_j^{(x_0)})$  を取得する。

## 【0026】

以上のように、k-out-of-n-OTや、数値属性に対して1-out-of-2 OTを用いて属性秘密鍵を配布することにより、ユーザ端末30は、自分の属性（kの値）を属性鍵管理サーバ10にも知られることなく、すなわち個人情報を全く漏らすことなく、当該自分の属性に対応する属性秘密鍵を取得することができる。

## 【0027】

## 2. 条件鍵の生成

プロバイダ端末20の条件鍵生成部22は、属性鍵管理サーバ10が公開している属性公開鍵を次に示すように組み合わせることによって、条件鍵を生成する。なお、 $E(PK, K)$ は、公開鍵PKでセッション鍵Kを暗号化することを示す。

(1) AND鍵の構成：属性条件 $A_i(v_{ij}) \& A_k(v_{kl})$ に対しては、それぞれ属性公開鍵 $y_{ij}$ 、 $y_{kl}$ が対応している。2つのセッション鍵 $K_{ij}$ 、 $K_{kl}$ をランダムに選び、これを公開鍵でそれぞれ暗号化すると条件鍵は $\{E(y_{ij}, K_{ij}), E(y_{kl}, K_{kl})\}$ となり、対応するセッション鍵は $K = K_{ij} + K_{kl}$ になる。この他、 $E(y_{ij}, E(y_{kl}, K))$ もANDを構成する暗号化になる。

(2) OR鍵の構成：属性条件 $A_i(v_{ij}) \mid A_k(v_{kl})$ に対しては、それぞれ属性公開鍵 $y_{ij}$ 、 $y_{kl}$ が対応している。セッション鍵Kの1つをランダムに選び、これを2つの公開鍵で暗号化する。条件鍵は $\{E(y_{ij}, K), E(y_{kl}, K)\}$ となる。

(3) NOT鍵の構成：属性条件 $\neg A_i(v_{ij})$ に対しては、属性公開鍵 $y_{ik}$ 、 $k = 1, \dots, j-1, j+1, \dots, n_i$ が対応している。セッション鍵Kを1つランダムに選び、これを $n_i - 1$ つの公開鍵で暗号化する。条件鍵は $E(y_{i1}, K) \parallel \dots \parallel E(y_{ij-1}, K) \parallel E(y_{ij+1}, K) \parallel \dots \parallel E(y_{ini}, K)$ となる。

(4) AND/ORの複合条件：上記を最下位レベルのオペレータから繰り返して、条件鍵をコンカテネートし、セッション鍵を計算していけば、任意のAND、ORの組み合わせに対する条件鍵およびセッション鍵を作ることができる。

## 【0028】

また、所定の  $n$  ビットの正整数  $Y = (y_{n-1}, \dots, y_0)$  に関して、 $X > Y$  が成立する場合にのみコンテンツを復号可能としたい場合を考える。プロバイダ端末 20 の条件鍵生成部 22 は、 $C = (c_{n-1}, \dots, c_0)$  を以下のようにして計算する。ここで、 $k_{n-1}, \dots, k_0$  は乱数とし、 $k_0 = K$  を数値属性条件 ( $X \geq Y$ ) に対するセッション鍵とする。次に、 $c_{n-1}, \dots, c_0$  を、以下のようにして決める。

$$c_j = E(s k_j^{(1)}, k_j) \quad \text{if } y_j = 1$$

$$c_j = E(s k_j^{(0)}, K) \parallel E(s k_j^{(1)}, k_j) \quad \text{if } y_j = 0$$

プロバイダ端末 20 は、 $(c_{n-1}, E_{k_{n-1}}(c_{n-2}), \dots, E_{k_1}(c_0))$  を条件鍵としてユーザ端末 30 へ送る。ユーザ端末 30 は、 $X \geq Y$  であれば、 $K$  が求まる。

同様の手法により、 $X > Y$ 、 $X \leq Y$ 、 $X < Y$  についても条件鍵を生成することができる。また、この手法による数値属性条件を組み合わせることにより、 $Y \leq X \leq Y'$  のような条件鍵を生成することもできる。

図 4 は、以上のプロトコルを説明する図である。

【0029】

### 3. マルチキャストによる配信

プロバイダ端末 20 は、上記の条件鍵生成プロトコルにて生成した条件鍵をコンテンツヘッダに付し、同じく上記条件鍵生成プロトコルにて生成したセッション鍵でコンテンツ本体を暗号化した上で、当該コンテンツヘッダ付きの暗号化コンテンツをマルチキャストする。図 5 は、このマルチキャストの様子を説明する図である。マルチキャストされたコンテンツは、条件鍵の条件に適合する属性秘密鍵を持つユーザ端末 30 だけが復号することができる。

【0030】

以上説明のように構成された本実施の形態による情報配信システムは、次に示すような大きな特徴を有する。

#### (1) 効率性および鍵取得のオフライン性：

ユーザ端末 30 は、属性鍵管理サーバ 10 から属性秘密鍵を受け取るが、これは 1 ラウンドのプロトコルで実現される。また、事前に一度、鍵取得をしておけ

ば、その後のマルチキャストに何回でも利用可能である。

(2) プロバイダ端末 2 0 の登録不要：

プロバイダ端末 2 0 は、属性鍵管理サーバ 1 0 の属性公開鍵を利用するが、この時、属性鍵管理サーバ 1 0 との対話は必要ない。また、属性公開鍵は再利用可能である。

(3) 属性鍵管理サーバ 1 0 のオフライン性：

属性鍵管理サーバ 1 0 は、ユーザ端末 3 0 の鍵取得時だけに関わり、実際の通信には関わらない。したがって、実際の通信では、IP マルチキャストなどの一般的なマルチキャストあるいはブロードキャストのプロトコルを使うことができる。

(4) 受信グループのオープン性：

マルチキャストによって、プロバイダ端末 2 0 は、受信者グループ及び受信可能な全体集合を知ることなく送信ができる。逆に言えば、ユーザ端末 3 0 は、任意の時間に属性鍵管理サーバ 1 0 から属性秘密鍵を受け取ることによって、受信可能グループに参加することができる。

【 0 0 3 1 】

次に、本実施の形態を適用可能な情報配信システムの具体例を説明する。

1：パーソナライズされた電子メール配信サービス

サービスプロバイダを介して複数のあるいは不特定のユーザに対して電子メールを配信するシステムがある。かかるシステムにおいて、サービスプロバイダ 7 0 0 が属性鍵管理サーバ 1 0 を運営し、電子メールの送信者 7 1 0 がプロバイダ端末 2 0 として、所定の属性に対応した条件鍵に基づいて暗号化された電子メールを配信することができる。図 7 に、かかるシステムの概略構成を示す。

本実施の形態によれば、電子メールの送信者は、電子メールの受信者の属性を特定するが、誰が特定された属性を持つかを知ることとはできないため、各ユーザの属性に関するプライバシーは完全に守られる。そのため、ユーザは安全に自分の属性に対する秘密鍵を取得し、パーソナライズされた情報を受け取ることができる。このシステムは、従来のデータベースマーケティングが、送信者側の類推によって受信者を選別していたモデルと異なり、受信者が自分の欲しい情報を能

動的に取ることができるため、よりヒット率の高い配信が可能になることが期待できる。

### 【 0 0 3 2 】

#### 2：分散マッチングサービスシステム

サービスプロバイダを介して複数のあるいは不特定のユーザ間で情報を照会し、交換するサービスがある。例えば、ネットワークを介したお見合サービスなどである。お見合サービスでは、会員であるユーザ間で交際条件及び自分のプロフィール情報を交換し、交換した情報に基づいて交際相手を捜すことが行われる。この場合、サービスプロバイダ 8 0 0 が属性鍵管理サーバ 1 0 を運営し、各ユーザの端末 8 1 0 がプロバイダ端末 2 0 及びユーザ端末 3 0 として機能する。そして、交換しようとする交際条件やプロフィール情報の項目を属性として指定し、当該属性に対応した条件鍵に基づいて暗号化されたメッセージをやり取りすることにより、互いの交換情報以外の情報を完全に秘匿したまま、情報交換を行うことが可能となる。図 8 に、かかるシステムの概略構成を示す。

### 【 0 0 3 3 】

#### 3：分散検索サービスシステム

検索エンジンの運営者が属性鍵管理サーバ 1 0 を運営し、属性として、専門分野などをキーワードとして登録しておく。ユーザ端末 3 0 は、自分の専門分野の属性秘密鍵を取得しておく。プロバイダ端末 2 0 に相当する質問者 9 1 0 が、質問をキーワードの組み合わせの形で設定し、ネットワークを介して配信する。すると、所定のユーザ端末 3 0 は、自分の専門に適合するときだけ、その質問を復号して見ることができ、質問に対する返答を行うことができる。図 9 にかかるシステムの概略構成を示す。

### 【 0 0 3 4 】

#### 4：コミュニティ鍵生成方式

図 1 0 に、本実施の形態による情報配信システムを用いたコミュニティ鍵生成方式の概略構成を示す。I S P (Internet Service Provider) などのネットワーク運営者が属性鍵管理サーバ 1 0 を運営する。そして、コミュニティのトピックを属性として登録しておく。コミュニティの会員は、プロバイダ端末 2 0 及び

ユーザ端末 30 として機能する端末装置 1010 を使用する。そして、ユーザ端末 30 としての機能により、自分の関心のあるトピックに対する属性秘密鍵を取得しておく。所定の会員は、自由に属性条件を組み合わせて、チャットルーム 1020 を開き、そのグループ鍵をメッセージとして生成し、当該属性条件に対応した条件鍵に基づき暗号化し、他の会員に配信する。これにより、当該属性条件に適合する受信者だけがグループ鍵を復号し、チャットルーム 1020 に参加できることとなる。なお、チャットルーム以外にも、ネットワーク上に置かれた種々のコンテンツを取得する鍵として条件鍵及び属性秘密鍵を設定できることは言うまでもない。

### 【0035】

#### 【発明の効果】

以上説明したように、本発明によれば、受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムにおいて、コンテンツの受け渡しに関わる全ての過程で、個人の属性情報が、送信者も含めた第三者に漏れないようにすることができる。

#### 【図面の簡単な説明】

【図 1】 本実施の形態による情報配信システムの概略構成を説明する図である。

【図 2】 本実施の形態における属性鍵管理サーバ、プロバイダ端末及びユーザ端末の構成を示す図である。

【図 3】 本実施の形態による k-out-of-n-OT による属性秘密鍵の配布プロトコルを説明する図である。

【図 4】 本実施の形態による条件鍵生成プロトコルを説明する図である。

【図 5】 本実施の形態によるコンテンツの配信の様子を示す図である。

【図 6】 本実施の形態による属性鍵管理サーバ、プロバイダ端末及びユーザ端末を実現するのに好適なコンピュータ装置のハードウェア構成の例を模式的に示した図である。

【図 7】 パーソナライズされた電子メール配信サービスシステムに本実施



の形態の情報配信システムを適用した構成を示す図である。

【図 8】 分散マッチングサービスシステムに本実施の形態の情報配信システムを適用した構成を示す図である。

【図 9】 分散検索に本実施の形態の情報配信システムを適用した構成を示す図である。

【図 1 0】 本実施の形態による情報配信システムを用いたコミュニティ鍵生成法式の概略構成を示すである。

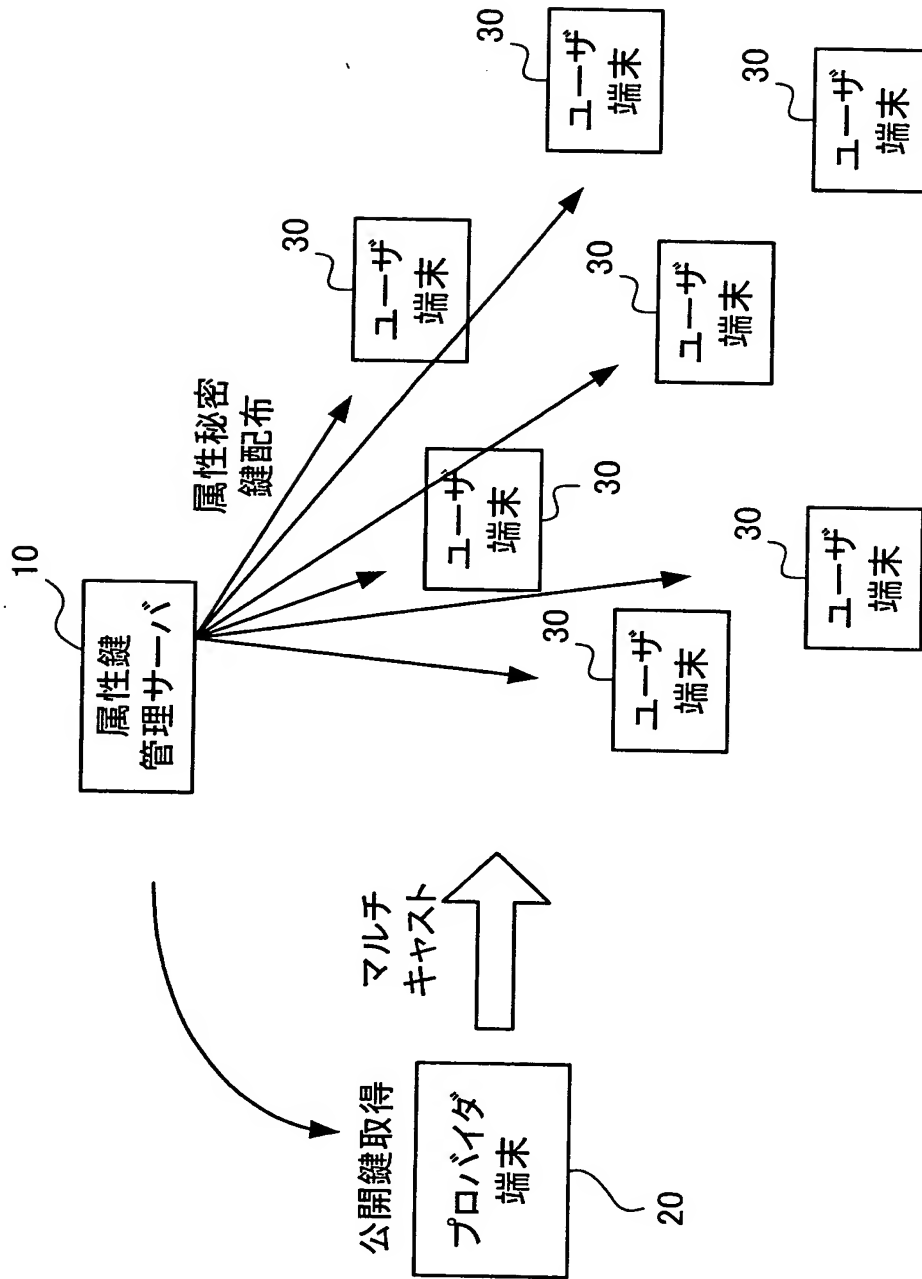
【符号の説明】

1 0 …属性鍵管理サーバ、 1 1 …属性鍵生成部、 1 2 …属性鍵格納部、 2 0 …プロバイダ端末、 2 1 …暗号化コンテンツ生成部、 2 2 …条件鍵生成部、 3 0 …ユーザ端末、 3 1 …属性秘密鍵格納部、 3 2 …復号処理部

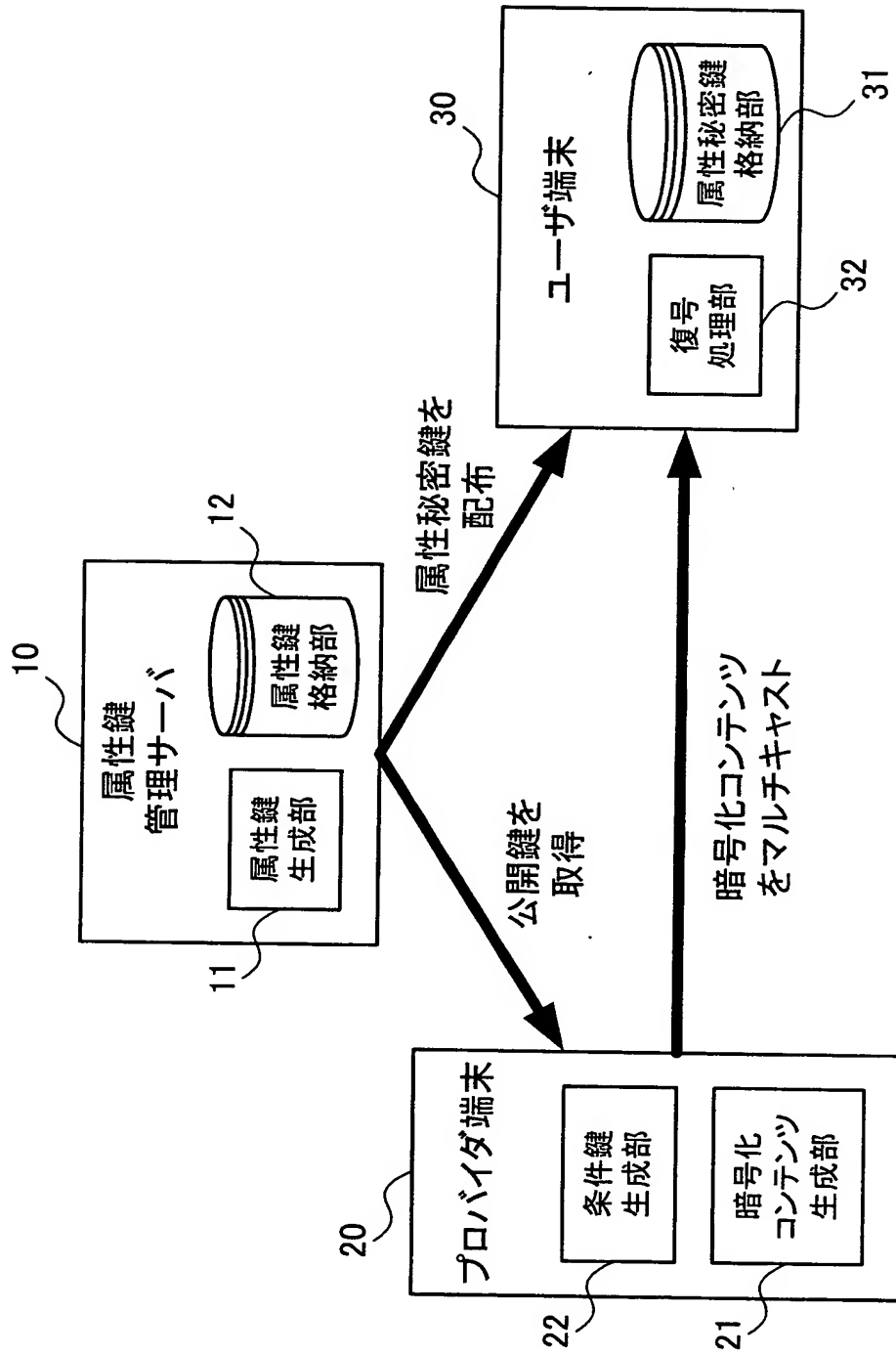
【書類名】

図面

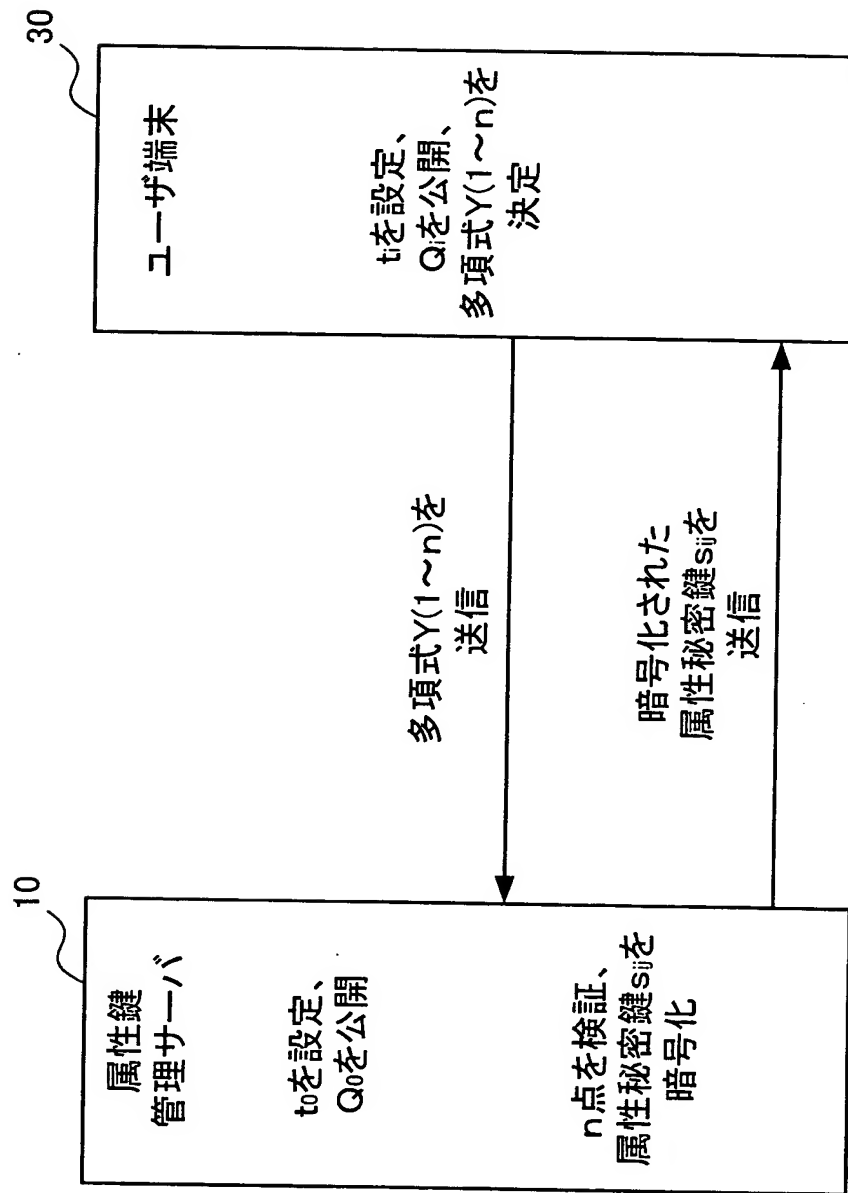
【図 1】



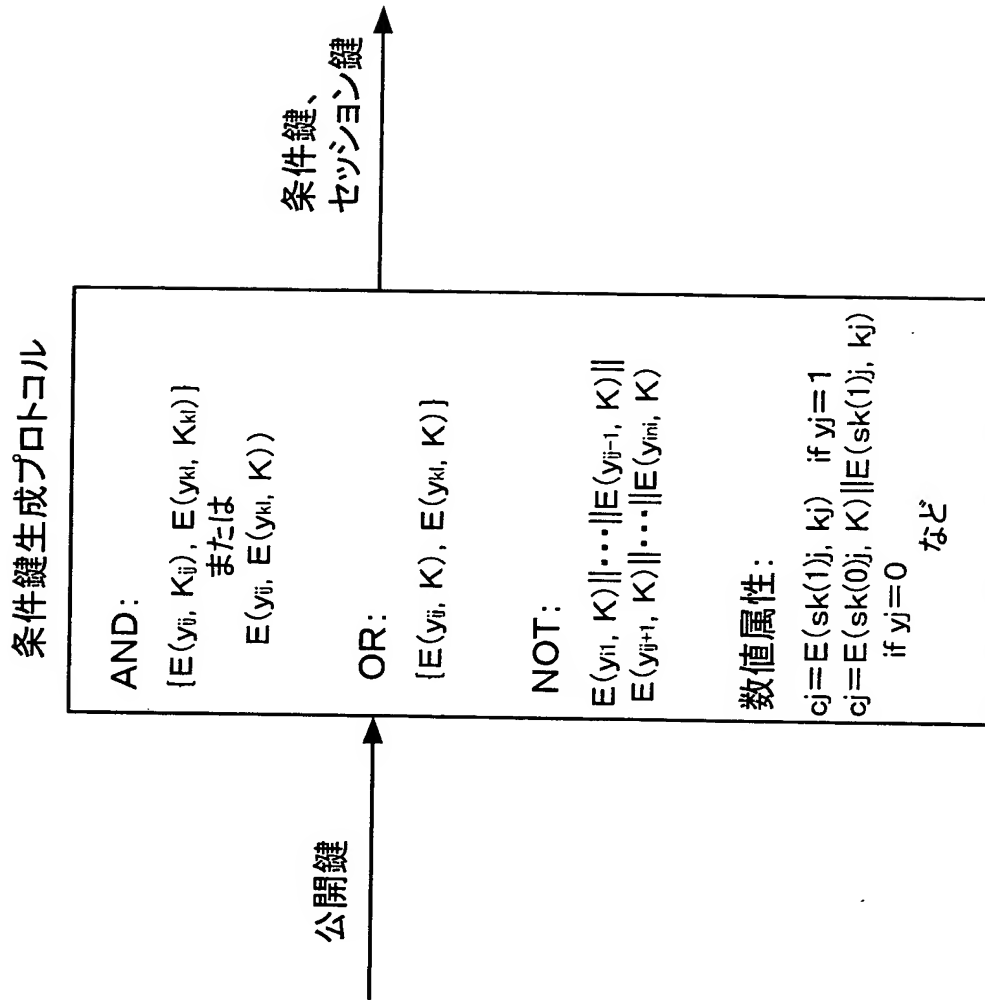
【図 2】



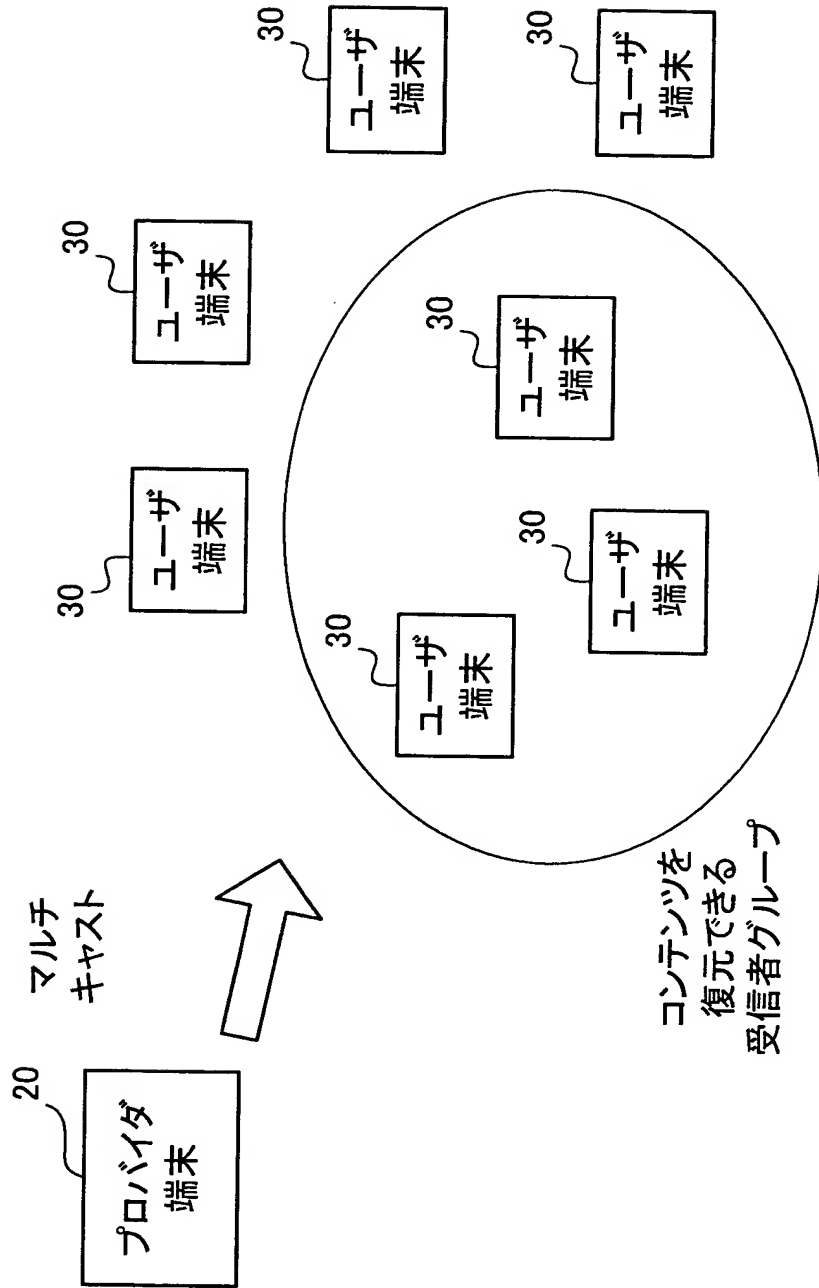
【図 3】



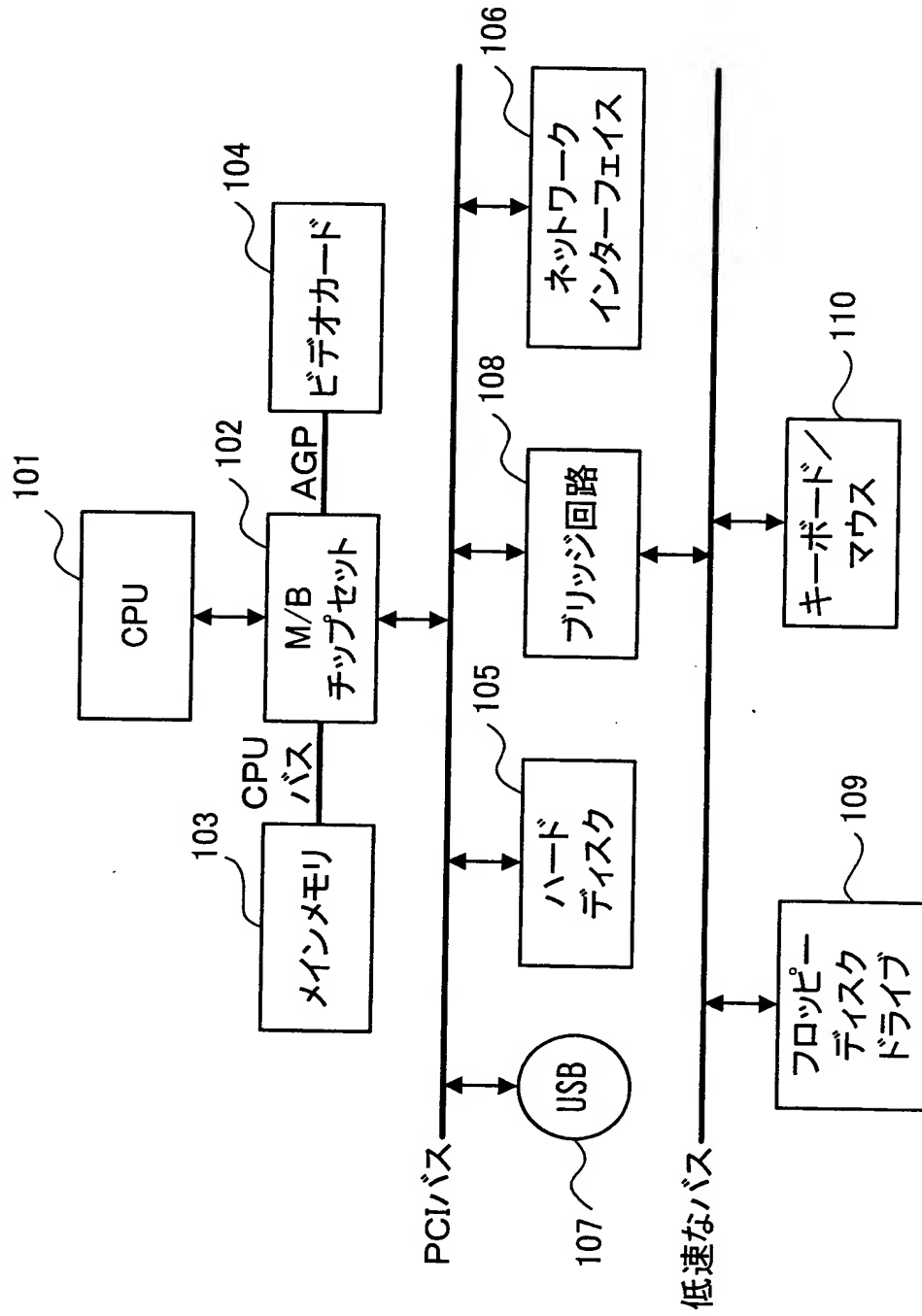
【図 4】



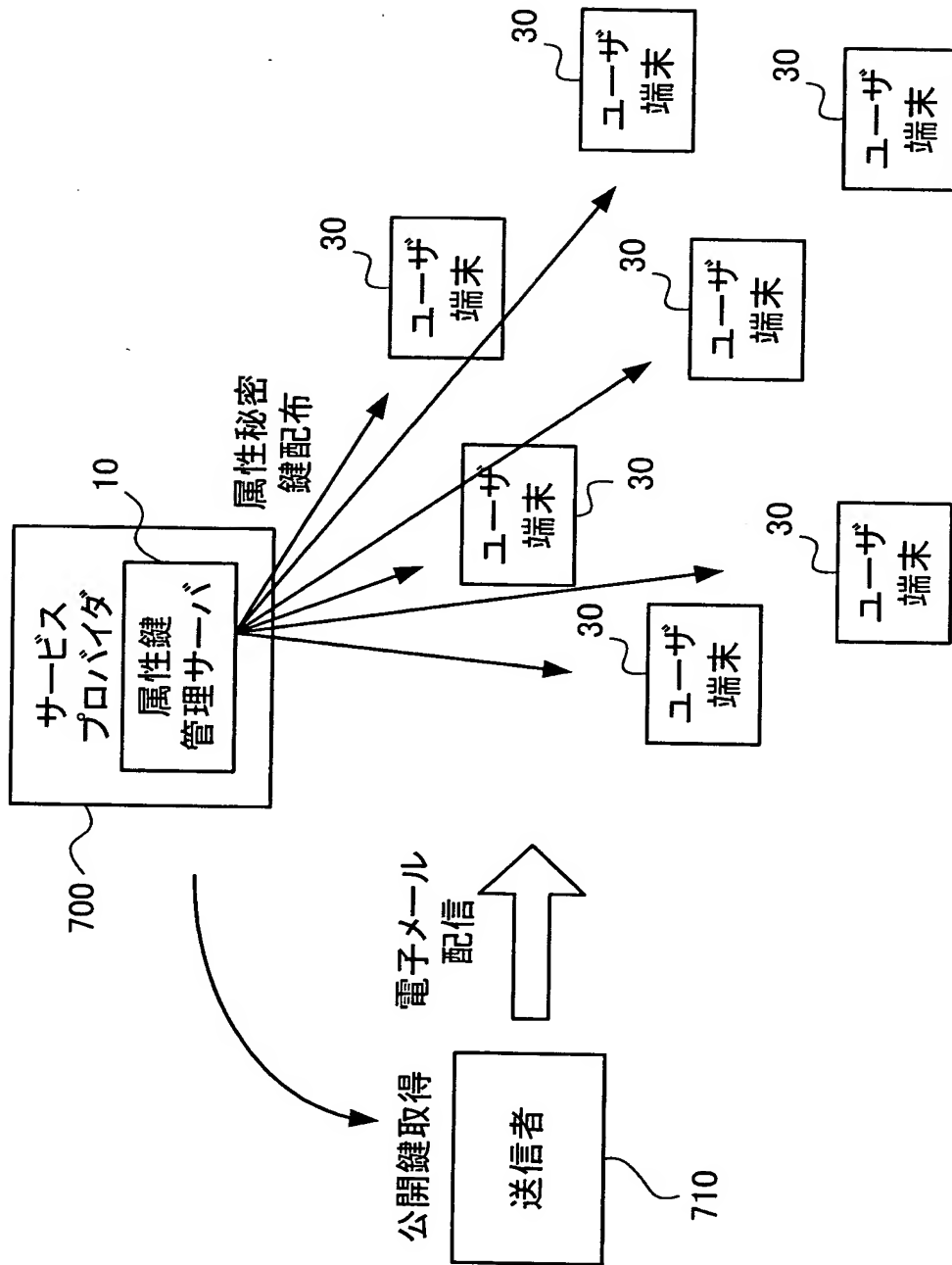
【図 5】



【図6】

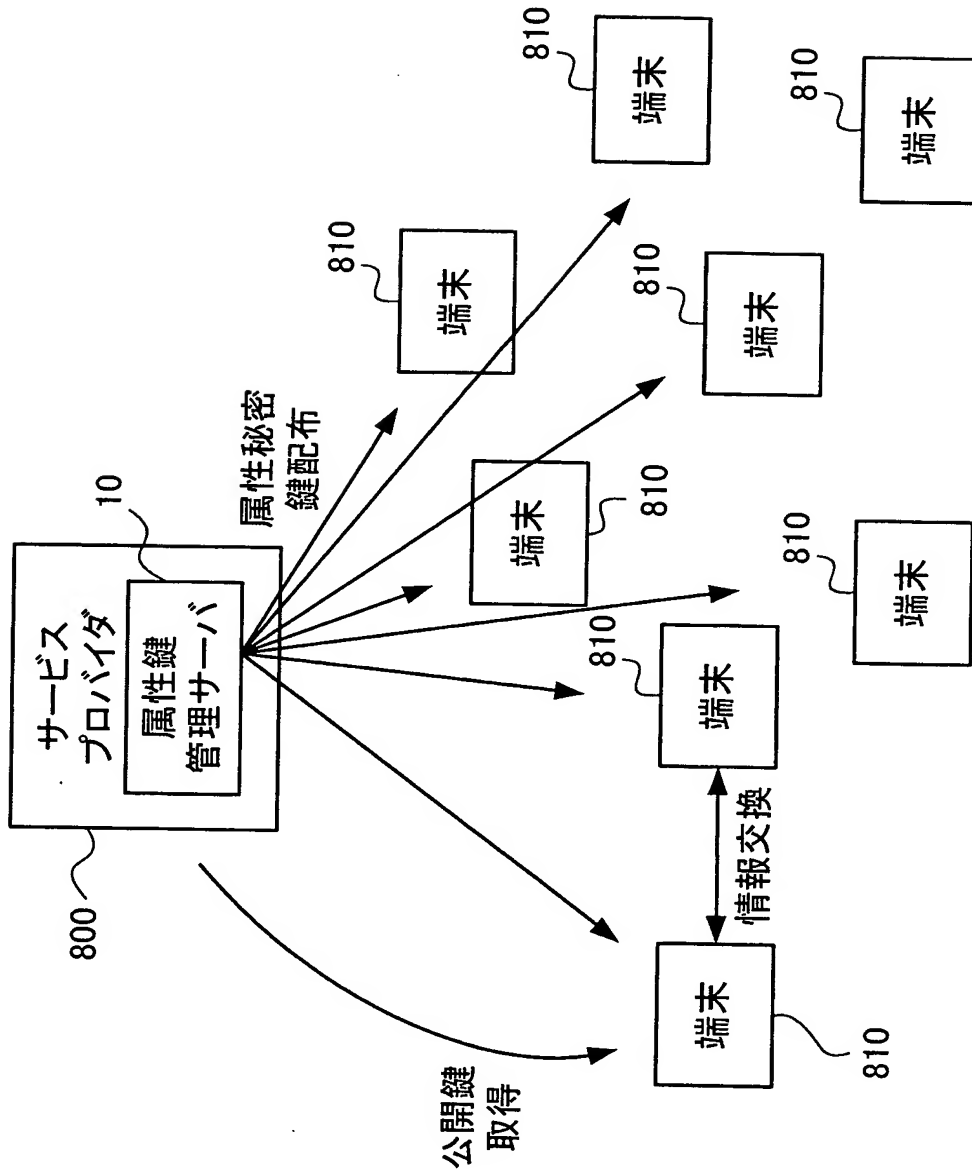


【図 7】

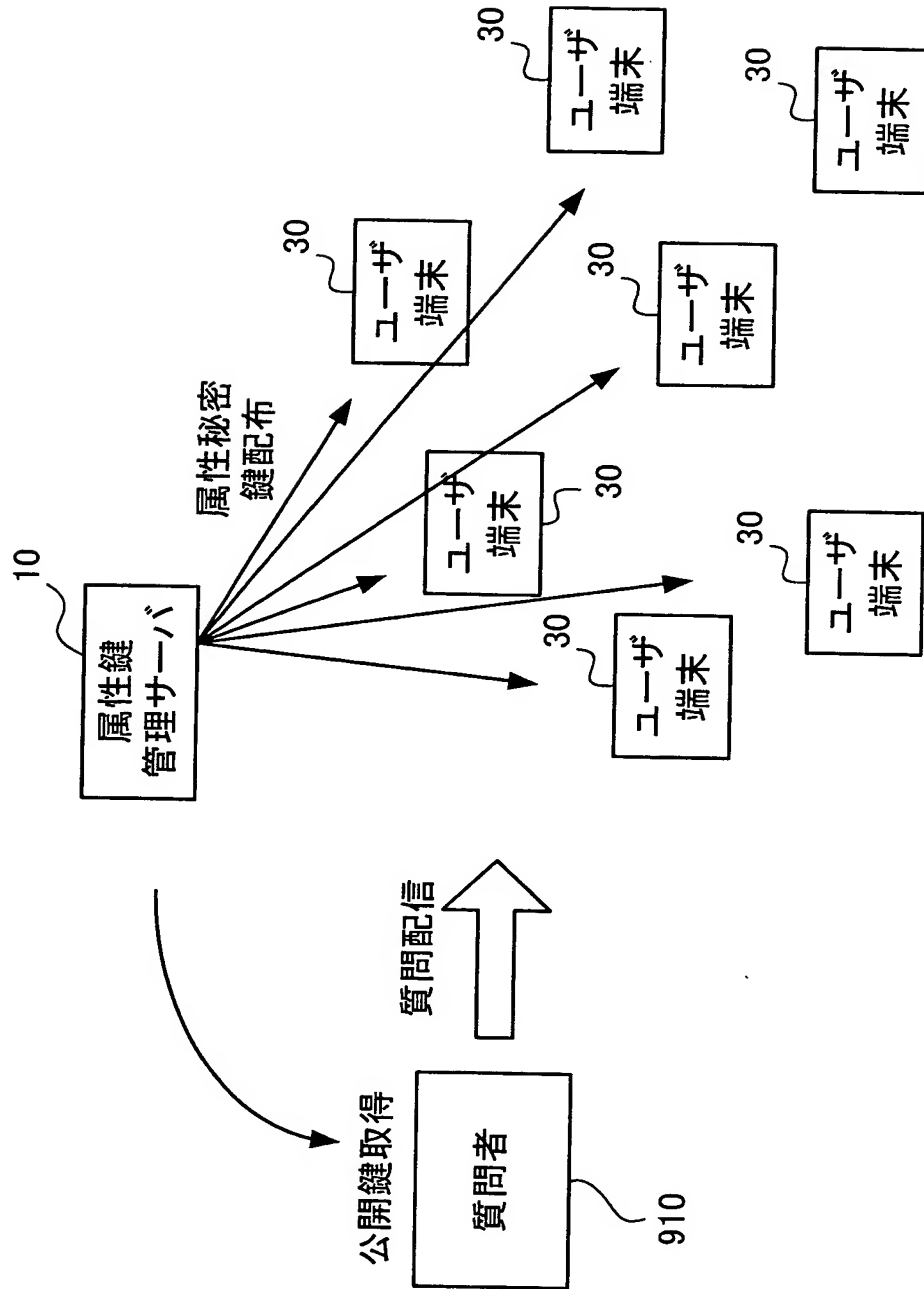




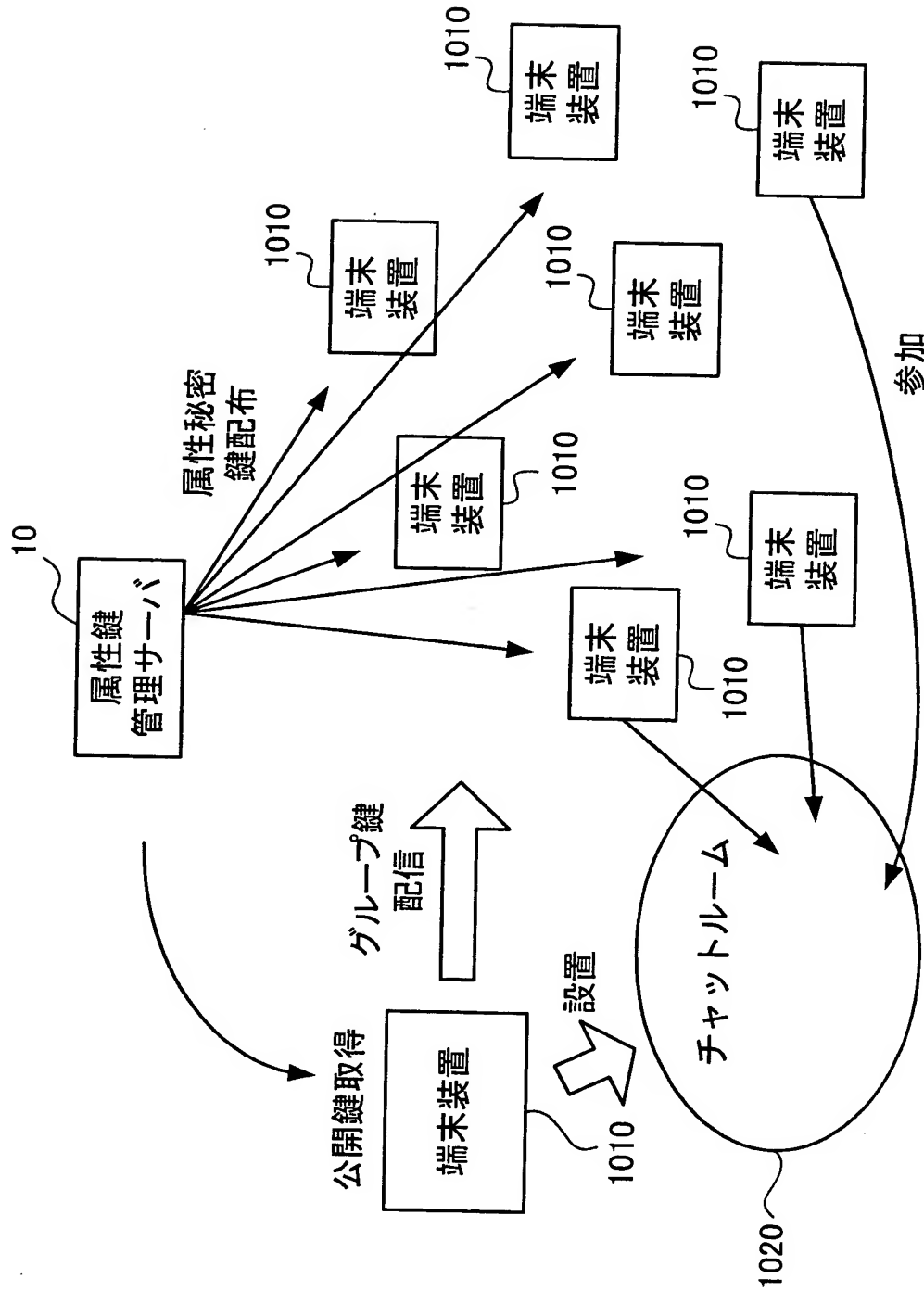
【図 8】



【図 9】



【図10】



【書類名】 要約書

【要約】

【課題】 受信者のアドレスを直接指定するのではなく、属性の組み合わせを条件として指定することによって、その条件を満たす人のみが受信できるような情報配信システムを提供する。

【解決手段】 所定の属性値に対する秘密鍵及び公開鍵を管理する属性鍵管理サーバ10と、この属性鍵管理サーバ10にアクセスし、秘密鍵に基づいて生成された自分の属性に対応する属性秘密鍵を取得するユーザ端末30と、公開鍵を用いて所定の属性に対する属性秘密鍵を持つユーザ端末30が復号可能な暗号化コンテンツを生成するプロバイダ端末20とを備える。そして、このプロバイダ端末20は、暗号化コンテンツを配信し、ユーザ端末30は、自分の属性秘密鍵にて復号可能な暗号化コンテンツを復号する。

【選択図】 図1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 2 - 1 8 3 5 1 1
受付番号	5 0 2 0 0 9 2 1 4 5 6
書類名	特許願
担当官	末武 実 1 9 1 2
作成日	平成 1 4 年 7 月 2 3 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	390009531
【住所又は居所】	アメリカ合衆国 1 0 5 0 4、ニューヨーク州 アーモンク ニュー オーチャード ロード
【氏名又は名称】	インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】	100086243
【住所又は居所】	神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	坂口 博

【代理人】

【識別番号】	100091568
【住所又は居所】	神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ビー・エム株式会社 大和事業所内
【氏名又は名称】	市位 嘉宏

【代理人】

【識別番号】	100106699
【住所又は居所】	東京都中央区日本橋本町 3 - 1 - 1 3 ロッツ和興ビル
【氏名又は名称】	渡部 弘道

【復代理人】

【識別番号】	100104880
【住所又は居所】	東京都港区赤坂 5 - 4 - 1 1 山口建設第 2 ビル 6 F セリオ国際特許事務所
【氏名又は名称】	古部 次郎

次頁無

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 2002年 6月 3日

[変更理由] 住所変更

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク ニ  
ュー オーチャード ロード

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレーショ  
ン